# Repeated Failures: What We Haven't Learned About Complex Systems

Patricia S. Vittitow[1]
*US Army Aviation and Missile Command (AMCOM); Huntsville Alabama, 35898*

**Several large-scale, high-risk programs have suffered catastrophic failures. Investigations have revealed numerous contributing factors. Starting with the Apollo 1 fire and the loss of the orbiters Challenger and Columbia, NASA has seen the greatest scrutiny due to the loss of life. The loss of the unmanned European Space Agency's Ariane 5 on its maiden voyage was a serious blow to the hitherto successful Ariane family of launch vehicles. The findings of the failure investigations can be grouped into general categories, some of which are common (e.g. process control) or unique to a particular accident (e.g. software design). Tabulating these causes has enabled assessing several large-scale weapons programs (either fielded or in development) as to commonality. Most of the weapons programs have experienced incidents of the general type, but without catastrophic results as yet. The question is raised: "Can this array of findings serve as a useful indicator for the weapons programs?"**

## I. Introduction

How do you assess the safety of an evolving, complex system, trying to be proactive without burdening the program unnecessarily? The catastrophic failures examined in this paper are from the National Aeronautical Space Administration (NASA) Shuttles Challenger and Columbia, Apollo 1 and the European Space Agency (ESA) Ariane 5 unmanned launch vehicle. The findings from these failures are then used to assess weapons programs which are in the process of fielding upgrades or still in the acquisition process in an attempt to determine the relative safety and effectiveness of the safety programs.

## II. Catastrophic Failures in Recent History

NASA has a systematic, documented safety process which failed to prevent two catastrophic Shuttle accidents because of lapses in following that process. Arianespace provided ESA the majority of its unmanned boost vehicles, and had a spectacular failure on the maiden launch of the Ariane 5—an upgrade to the long-successful Ariane 4. Military programs, especially those using new or a mixture of new and existing technologies, often suffer from the lack of a structured safety review process (such as used by NASA), a problem which is compounded by the need to field a system quickly to meet emerging threats. Few, if any programs, look to capitalize on the painful knowledge gained from the following program failures.

*Apollo 1*: The on-pad fire in the Apollo 204 Command Module (later renamed Apollo 1) occurred during an operational check-out procedure designed to demonstrate all space vehicle systems and operational procedures in as near a flight configuration as was practical. The cause of the fire and subsequent rupture of the module was detailed in a Presidential Report. Best assessment is that an electrical arc occurred in the lower forward section of the left-hand equipment bay. This was coupled with the secondary finding of excessive combustible materials and a hazardous test environment of 100 percent oxygen. Between the flash fire and the release of toxic gasses, the crew was unable to perform an emergency egress. Once the module ruptured, rescue personnel were unable to assist the crew due to the release of toxic fumes and heat from the module (no special equipment was readily available) contaminating the "White Room."

[1] Safety Chief, *US Army Aviation and Missile Command (AMCOM)*, BLDG 5301 ATTN: AMSAM-SF

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **NOV 2010** | | **00-00-2010 to 00-00-2010** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Repeated Failures: What We Haven't Learned About Complex Systems** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Army Aviation and Missile Command (AMCOM),ATTN: AMSAM-SF,BLDG 5301,Huntsville,AL,35898** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES
**See also ADM202978. Presented at the AIAA Missile Sciences Conference Held in Monterey, California on November 16-18, 2010. Sponsored by the Office of the Under Secretary of Defense, Acquisition Resources and Analysis Security Management.**

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **Same as Report (SAR)** | **24** | |

Lessons Learn from Apollo 1:

- System design was not robust with regards to wire/cable design and insulation. Combustible materials and power lines were in unacceptable proximity. Coupled with the 100 percent oxygen, the test environment was too hazardous.
- Deficiencies existed in Command Module design, workmanship and quality control.

*Challenger*: The 25th Space Shuttle mission ended at T+73 seconds when the vehicle exploded. After the explosion of the external tank, the Orbiter vehicle was torn apart by the subsequent loads and the resultant activation of the Flight Termination System (FTS) on the Solid Rocket Boosters (SRB).

The Presidential Commission on the Challenger Accident (the Rogers Commission) fairly quickly determined the hardware failure mechanism, and in doing so uncovered larger programmatic factors that directly led to the loss of the mission and its seven member crew. The primary failure was a combustion gas leak through the right SRB aft field joint that weakened/penetrated the External Tank (ET), resulting in an explosion and subsequent structural failure. The gas leak was the result of a single o-ring field joint design. Low temperatures led to loss of o-ring resiliency, exacerbated by an out-of-round condition of those reusable motor segments, which allowed a gap to remain or even open wider rather than close due to motor ignition pressures. The location of the leak allowed it to impinge on the ET, and either directly or indirectly led to the failure of the hydrogen tank, located in the lower half of the ET. The gas also impinged on the lower struts which connect the SRB to the ET. The single thrust post connection at the forward SRB/ET attachment then acted as a pivot point responding to the SRB thrust, pushing the nose of the SRB into the lower part of the oxygen tank in the inter-tank section of the ET. The resultant explosive burn enveloped the Orbiter and ignited its reaction control system propellants. Under severe loads, the Orbiter broke apart into large segments, the ET into smaller pieces, and the now separated SRB's were terminated using the FTS.

Lessons Learned from Challenger:

- A faulty design was allowed to continue in use despite documented near-misses. This includes a design unacceptably sensitive to the effects of temperature, physical dimensions, character of materials, effects of reusability, processing and the reaction of the joint to dynamic loading.
- Waiving of launch constraints at the expense of flight safety. There was no system in place which made it imperative that launch constraints and waivers of launch constraints be considered by all levels of management.
- A propensity of management at one center to contain potentially serious problems and to attempt to resolve them internally rather than communicate them forward.

*Ariane 5*: The maiden flight of the Ariane 5 launcher lasted 40 seconds, at which point the vehicle veered off course, and broke up due to loads and subsequent initiation of the FTS system when links between the solid rocket booster and the core stage were severed.

The Ariane 5 is a non-man rated launch vehicle consisting of two solid propellant motors, each with three segments and a cryogenic liquid engine. These solid motors are attached to the sides of the main cryogenic core stage containing the Vulcain engine. Each solid motor contains 237 metric tons of propellant. The On-Board Computer (OBC) ordered full nozzle deflection for both solid rocket motors and the Vulcain at approximately T+39 seconds. This was based on data received from the active Inertial Reference System (SRI), one of two identical systems. One is active while the other is in stand-by mode in the event of failure. On this flight, however, the back-up SRI had already failed due to a software exception—the same one which 72 milliseconds later took out the primary. The exception was caused when a data conversion from a 64-bit floating point to a 16-bit signed integer failed. This error actually occurred in a section of code which was only designed to operate on the ground, and was timed for Ariane 4 launches. At the time that code was carried over from Ariane 4 to Ariane 5, this software module was left enabled for the first 40 seconds of flight. This was to allow easier reset in the event of a very late abort, but only useable by Ariane 4. The result was that the SRIs, running the same code and receiving the same inputs, shut themselves down because of the operand failure. The final data sent to the OBC was essentially diagnostic data, but was interpreted as flight data. This resulted in the attempted correction of a perceived attitude deviation which in fact had never occurred. Aerodynamic loads caused one or both solid rocket boosters to pull away from the cryogenic core, which activated the FTS system, terminating the launch.

Lessons Learned/Recommendations from Ariane 5:

- No software function should run during flight unless it is needed.

- Perform complete, closed-loop system testing. Complete simulations must take place before any mission.
- Review all flight software (including embedded software) to identify all implicit assumptions made by the code and its justification documents on the values of quantities provided by the equipment. Verify the range of values taken by internal or communication variables in the software.
- Review the test coverage of existing equipment and extend it where it is deemed necessary

*Columbia*: Approximately 16 minutes from touchdown, the Space Shuttle Columbia broke up in the upper atmosphere, with the loss of seven crewmembers. Foam from the External Tank had broken off during launch and impacted the leading edge of the left wing. Weakened, this area failed during the thermal stresses of re-entry, resulting in loss of control and vehicle break-up due to the wing melting and subsequent loss of control system located internal to the wing.

As with the Challenger Investigation, the Accident Investigation Board found non-hardware contributors to the accident. The final report documented numerous very specific findings related to the thermal protection system, sensors and other shuttle-unique items.

Lessons Learned/Recommendations from Columbia:

- Adopt and maintain a (Shuttle) flight schedule that is consistent with available resources. Although schedule deadlines are an important management tool, those deadlines must be regularly evaluated to ensure that any additional risk incurred to meet the schedule is recognized, understood, and acceptable
- Implement an expanded training program in which the Mission Management Team faces potential crew and vehicle safety contingencies beyond launch and ascent.
- Establish an independent Technical Engineering Authority that is responsible for technical requirements and all waivers to them, and will build a disciplined, systematic approach to identifying, analyzing and controlling hazards throughout the life cycle of the [Shuttle] System.
- NASA Headquarters Office of Safety and Mission Assurance should have direct line authority over the entire Space Shuttle Program safety organization and should be independently resourced.
- Reorganize the Space Shuttle Integration Office and make it capable of integrating all elements of the Space Shuttle Program, including the orbiter
- Prepare a detailed plan for defining, establishing, transitioning, and implementing an independent Technical Engineering Authority, independent safety program, and a reorganized Space Shuttle Integration Office as described in previous recommendations. In addition, NASA should submit annual reports to Congress, as a part of the budget review process, on its implementation activities.

## III. Findings Summary

Table 1 categorizes the findings of the previously discussed catastrophic failures. It should be noted that not all findings were included in this paper. This is most notable with the Challenger and Columbia findings. Predominantly only the more generic, that is not NASA-specific, were included.

The broad-brush categories were selected to provide the most flexible categorization of issue or failure, in order to be usable across the greatest spectrum of programs or products. The one category which could be added when dealing with military programs is acquisition acceleration. The global threat environment more acutely impacts the fielding of weapons systems, requiring shorter design, development and release processes than have been seen historically. Spiral Development, which accepts that capability lags behind production in the early years, is being used by the Department of Defense (DoD) for some critical weapons systems. The Ground-Based Midcourse Defense (GMD) is one such large-scale program using spiral development. Other programs, such as the Patriot Advanced Capability – 3 (PAC-3) is continually making improvements over the initial Patriot fielding, but using a more typical DoD acquisition process. In theory, the commercial aviation and aeronautics community does not have the driver of national security to make it short circuit the normal design process, and hence potentially the safety process.

Table 1 – Categorized Findings

| Finding Category | Apollo 1 | Challenger | Columbia | Ariane 5 |
|---|---|---|---|---|
| Communication | | ✓ | | |
| Hardware Design | ✓ | ✓ | ✓ | |
| Independent Review | | | | ✓ |
| Management | | ✓ | ✓ | |
| Process Control | ✓ | ✓ | ✓ | ✓ |
| Safety Culture | | ✓ | ✓ | |
| Software Design | | | | ✓ |
| Test Set-up | ✓ | | | ✓ |
| Training | | | ✓ | |
| Workmanship/Quality Control | ✓ | | | |

### *Current Case Studies*

Using some current weapon systems, a new matrix was developed adding these in an additional column (Table 2). These systems are either fielded but undergoing upgrades, or in the final test phases prior to release.

Table 2 – Categorized Findings with Case Studies

| Finding Category | Apollo 1 | Challenger | Columbia | Ariane 5 | Military Systems |
|---|---|---|---|---|---|
| Communication | | ✓ | | | ✓ |
| Hardware Design | ✓ | ✓ | ✓ | | ✓ |
| Independent Review | | | | ✓ | ✓ |
| Management | | ✓ | ✓ | | ✓ |
| Process Control | ✓ | ✓ | ✓ | ✓ | ✓ |
| Safety Culture | | ✓ | ✓ | | ✓ |
| Software Design | | | | ✓ | ✓ |
| Test Set-up | ✓ | | | ✓ | ✓ |
| Training | | | ✓ | | ✓ |
| Workmanship/Quality Control | ✓ | | | | ✓ |

Program documentation supports that all of the assessed military programs have at some point experienced more than one of the finding categories and in some programs all finding categories were present in one system.

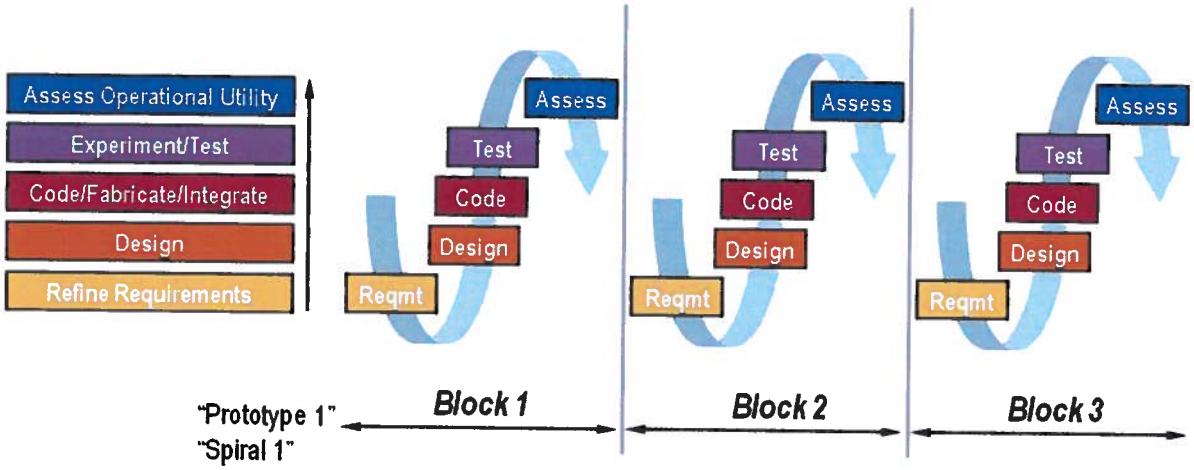
Some of the military programs assessed include not just a weapon element, but also an integrated radar system. Earlier versions of these systems relied on manual or procedural controls for redundancy. In a hostile threat environment, those controls often broke down. One well-known incident involved the mistaken shoot-down of a civilian airliner, with the loss of all on board. Initial findings were that un-user friendly displays (software, hardware design), ground-to-air communications (hardware design, communication) as well as safety culture and process

control were contributors to the tragedy. The system has since been upgraded, but is now being incorporated as part of a larger military program, with more interfaces and interactions. Using the previously identified findings is a logical place to start the assessment of the system as it evolves towards the expanded mission.

Another integrated weapons system was responsible for multiple friendly-fire casualties, as well as being a target itself of friendly-fire. Initial findings for these incidents included software and hardware design, communication and training. Again, multiple hits on the general findings matrix. Procedural controls were immediately implemented to prevent further losses. This was a "soft" fix to a problem which is on the list for long-term remediation.

Programs currently in development have been assessed against the findings matrix. However, these programs have not had an operational – related fatality. Why? Several reasons exist, which could include an experienced Prime Contractor(s), limited, but perhaps most telling, the fact that they are not yet a fielded system. Findings by independent review board(s) into various aspects of these military programs focused on quality/workmanship, hardware and software design and process control. All of these represent potential safety impacts. The programs are forced to conduct flight tests, integrate and emplace tactical hardware while trying to continue to improve via the spiral development process. Tracking and monitoring of findings as the program responds to a heightened threat environment may help manage scarce resources (funding, personnel) by allowing for better risk assessment and management.

As mention earlier, another contributing factor to some of these issues being present in systems and demonstrating very clearly the need to learn from past lessons is systems being developed under "spiral development." A notional spiral development is depicted in the following diagram.




Couple spiral development acquisition with urgent fielding of a system further exacerbates problems. Many safety features (as well as performance) are most effective, performance and cost perspective, if implemented in the basic design. It may appear to be cost effective to delay key safety elements into future block upgrades (with appropriate risk acceptance) until accidents occur upon fielding, equipment is "dead lined", taken out of service, procedures must be revised, etc. Spiraling in new development almost always requires additional and expensive re-qualification testing. It is often times difficult for the Warfighter to determine the differences in upgrades between the spirals thus adding to confusion.

Using these lessons learned from failures in other complex systems can also aid in evaluating new designs at both the preliminary design reviews and critical design reviews. Often times, the contrast of what is on paper at design reviews with what is reality is best illustrated in the list below:

| "On Paper" | Reality |
|---|---|
| ▪ It is simple. | ▪ It is complicated. |
| ▪ It is small. | ▪ It is large. |
| ▪ It is cheap. | ▪ It is expensive. |
| ▪ It is lightweight. | ▪ It is heavy. |
| ▪ It can be built very quickly. | ▪ It takes a long time to build because of its engineering development problems. |
| ▪ Very little development is required; it can use off-the shelf components. | ▪ It requires an immense amount of development on apparently trivial items. |
| ▪ It is in the study phase; it is not being built now. | ▪ It is being built now. |

While the above list is humorous to read it is sadly too often the case during system development.

This is meant to be a qualitative approach to an assessment, thus there is no magical number of findings or factors which would put a program at risk. Would the friendly fire incidents have been avoided if such an assessment had been made? Probably not – we were either directly or indirectly involved in an armed conflict. However, using the generic findings as a running state of the program assessment can give you visibility of those areas that need immediate remediation, either as a short term fix (procedures, training) or the preferred long-term solution (hardware and software upgrades, re-establishment of a healthy safety culture).

## IV. Conclusion/Recommendations

The complexity of many of today's large-scale programs currently works to safety's advantage. However, that complicates sending the message that there are significant safety findings which need resolution prior to release to the Warfighter. System safety is not risk-adverse, per se, but risks should be documented, assessed, mitigated where possible and if not mitigated, then processed as a residual risk accepted at the appropriate level. To do less is to accept risk without understanding the impact and avoiding tough decisions.

A thorough scrutiny of a program as it exists—a comparison of what it should be and what it actually is with regards to safety compliance—is needed for the near term operations such as more complicated demonstrations, salvo test launches, system upgrades and to the eventual transition to a Warfighter as an operational system. In some recent specific systems failures during test flights have led to the impression that the system is more likely to fail to launch than not – a valid concern with serious consequences in time of need. In fact, from a Warfighter stand-point, failure to launch when needed is the top hazard – a reversal of the standard safety position.

A healthy safety culture would be to surface issues for resolution, whether it be corrections to the hardware/software/process, or the documenting of residual risks to assure all involved parties are aware and make a conscious decision to accept the risk. The Warfighter understands that spiral development results in a system which is constantly maturing but deserves to receive full disclosure of capabilities, limitations and risks as he prepares to use the system.

## Acknowledgments

The author would like to acknowledge contributions to this paper by Ms. Susan Cantrell, Senior Safety Engineer, A-P-T Research, Inc., 4950 Research Drive, Huntsville, AL 35805 Her assistance was invaluable in reducing the NASA incidents "lessons learned" to those that would be applicable to DoD systems. A large portion of Ms Cantrell's experience was in support of NASA's Marshall Space Flight Center and Glenn Research Center - Fault Tree Analysis of the Solid Rocket Booster for the STS-26 return to flight, development of safety data packages for Shuttle and Space Station payloads and joint US-Russian missions to Mir. She worked at the European Space Agency in the In-Orbit Technology Demonstration Program, which developed Shuttle-based microgravity

experiments. Leaving the NASA world, she performed hazard assessments and inspections on Army Tactical Operations Centers prior to joining A-P-T Research Inc.

## References


[1] Apollo 1: Apollo 204 Review Board, April 5, 1967, NASA Historical Reference Collection, NASA History Office, NASA HQ, Washington, DC

[2] Challenger: Presidential Commission Report on the Challenger Accident; June 6, 1986, NASA Historical Reference Collection, NASA History Office, NASA HQ, Washington, DC

[3] Ariane: Ariane 5 Flight 501 Failure: Report by the Inquiry Board, Dated 19 July 1996, European Space Agency, Paris, France.

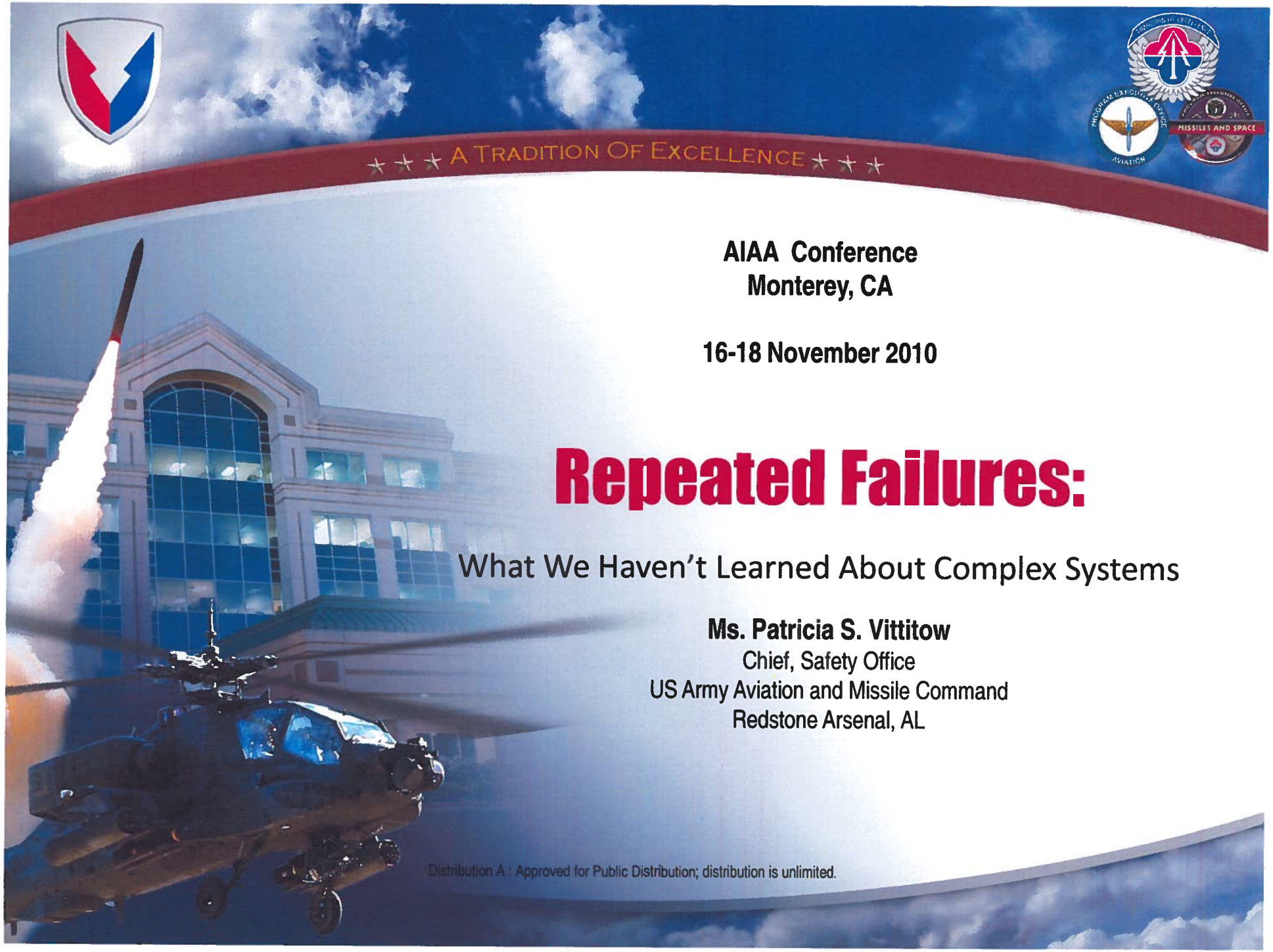
[4] Columbia: Columbia Accident Investigation Board Final Report, August 2003, NASA Historical Reference Collection, NASA History Office, NASA HQ, Washington, DC

[5] Paper, Michael D. Griffin, 61st International Astronautical Congress, September 2010, titled: "How Do We Fix System Engineering?"


## Biographies


P.S. Vittitow, BSChE, MSChE, MBA; Chief, AMCOM Safety Office, AMSAM-SF, Redstone Arsenal, Huntsville, AL, 35898-5130, USA, telephone 256-876-2944, fax 256-842-8643, e-mail: Patricia.Vittitow@us.army.mil


Patricia Vittitow, currently the Chief of the Safety Office for the US Army Aviation and Missile Command, Redstone Arsenal, Huntsville, AL, has spent her 30 years in government service in the safety arena -in system safety, explosive safety, hazard classification, insensitive munitions, operational/production safety, and safety training. She is responsible for the safety material release and system safety for all Army missile and aviation systems, and operational safety for AMCOM at Redstone Arsenal, Corpus Christi Army Depot and Letterkenny Army Depot. Prior to her current position, she was the Safety Director at the US Army Space and Missile Defense Command and her work revolved around large missile systems such as the Ground Based Midcourse Defense Program, THAAD, and PAC-3. She is a recognized expert in large rocket motors. She is a past board Chairman of the US Army IM Board and a member for 14 years. Ms. Vittitow has received numerous awards including the Civilian Meritorious Award, Commander's Award, and IM Achievement Award. She has a BS in Chemical Engineering, an MSE and an MBA from the University of Louisville.




**AIAA Conference**
**Monterey, CA**

**16-18 November 2010**

# Repeated Failures:

## What We Haven't Learned About Complex Systems

**Ms. Patricia S. Vittitow**
Chief, Safety Office
US Army Aviation and Missile Command
Redstone Arsenal, AL

# Introduction

A TRADITION OF EXCELLENCE

- Today's complex Military systems are constantly evolving and adapting to emerging threats and acquisition strategies
- System Safety must be able to assess hardware and software outside of a typical structured review environment
- Developer goals and Warfighter safety may be at odds with each other

# Paper Intent

A TRADITION OF EXCELLENCE

- Determine if assessment against historical findings categories could:
  - Assist in assessment of fielded systems which face upgrades and evolution in mission
  - Provide a baseline/tool to better assess systems using spiral development (lack of traditional program milestone reviews, tests and materiel release process)

# Paper Methodology

A TRADITION OF EXCELLENCE

- Catastrophic failures of large scale systems have well-documented findings
- Findings grouped into 10 general categories
- Review of systems in development or fielding/upgrades found parallels in major and minor incidents to historical studies

| *Finding Category* | *Apollo 1* | *Challenger* | *Columbia* | *Ariane 5* | *DOD Weapon Systems* |
|---|---|---|---|---|---|
| **Communication** | | | | | |
| **Hardware Design** | | | | | |
| **Independent Review** | | | | | |
| **Management** | | | | | |
| **Process Control** | | | | | |
| **Safety Culture** | | | | | |
| **Software Design** | | | | | |
| **Test Set-up** | | | | | |
| **Training** | | | | | |
| **Workmanship/Quality Control** | | | | | |

# Paper Methodology



- Catastrophic failures of large scale systems have well-documented findings
- Findings grouped into 10 general categories
- Review of systems in development or fielding/upgrades found parallels in major and minor incidents to historical studies

| Finding Category | Apollo 1 | Challenger | Columbia | Ariane 5 | DOD Weapon Systems |
|---|---|---|---|---|---|
| Communication | | ✓ | | | ✓ |
| Hardware Design | ✓ | ✓ | ✓ | | ✓ |
| Independent Review | | | | ✓ | ✓ |
| Management | | ✓ | ✓ | | ✓ |
| Process Control | ✓ | ✓ | ✓ | ✓ | ✓ |
| Safety Culture | | ✓ | ✓ | | ✓ |
| Software Design | | | | ✓ | ✓ |
| Test Set-up | ✓ | | | ✓ | ✓ |
| Training | | | ✓ | | ✓ |
| Workmanship/Quality Control | ✓ | | | | ✓ |

# Apollo 1 Findings

A TRADITION OF EXCELLENCE

## What happened:

- Best assessment is electrical arcing occurred in an equipment bay in conjunction with:
  - Excessive combustible materials
  - Hazardous 100% $O_2$ cabin environment
  - A flash fire released toxic gases, which combined prevented the crew from performing an emergency egress
  - Subsequent Command Module rupture contaminated the "White Room," preventing rescuers from reaching the crew

- Hardware Design
  - System design, especially with regards to wire/cable design & insulation was not robust
  - Combustible materials and power lines routed in proximity
- Test Set-up
  - Hazardous test environment of 100% $O_2$
- Workmanship/QC:
  - Deficiencies in CM design, workmanship and quality control

# Challenger Findings

A TRADITION OF EXCELLENCE

## *What happened:*

- Failure of Solid Rocket Motor (SRM) field joint allowed hot gases to impinge on External Tank (ET) and lower struts (aft attach points between ET and Solid Rocket Booster (SRB)) Hydrogen tank rupture occurred due to direct or indirect impingement
- SRB nose ruptured the Oxygen tank when forward attach point acted as a pivot point once the rear attach points failed
- Resultant ET explosions engulfed the Orbiter and ignited the reaction control propellants
- Severe loads caused break-up of the Orbiter, and the SRB's were terminated via Flight Termination System (FTS)

- Communication
  - Compartmentalization of information
- Hardware Design
  - Faulty design allowed to remain in use despite documented near-misses
- Management
  - Waiving of launch constraints, with no system in place to require review of waivers at management levels
- Process Control
  - Process did not account for identification of problems that surfaced during refurbishments
- Safety Culture
  - Inability to raise safety issues to appropriate level

# Columbia Findings

A TRADITION OF EXCELLENCE

## What happened:

- During re-entry, damage from foam debris at launch allowed the underside of the left wing to be breached, with subsequent vehicle break-up and loss of seven crew members

- Hardware Design
  - ET Foam unduly sensitive
- Management
  - Unrealistic flight schedules given available resources
  - Reorganize the shuttle Integration Office to include all elements
- Process Control
  - Establish an independent Technical Engineering Authority which would manage hazards throughout shuttle system
  - Foam installation & inspection
- Safety Culture
  - NASA Office of Safety & Mission Assurance to have direct line authority over shuttle safety program, independently resourced
- Training
  - Expand training for crew and vehicle contingencies

# Ariane 5 Findings

A TRADITION OF EXCELLENCE

## What happened:

- Maiden flight of Ariane 5 lasted 40 seconds, when vehicle broke-up due to loads and FTS activation
  - Legacy software remained though not useable by Ariane 5
  - Single operand failure caused both navigational computers to auto-shutdown

- Independent Review
  - Review all software, including imbedded code to validate assumptions
- Process Control
  - Design and testing processes not synchronized
- Software Design
  - No software function should run during flight unless needed (corollary: no dead code)
- Test Set-Up
  - No complete, closed-loop testing performed; full simulation required before each mission
  - Review test coverage of existing equipment and extend where necessary

# DOD Findings

A TRADITION OF EXCELLENCE

- Communication
  - "Tabling" of non-compliances i.e. no acceptance of residual risks
  - Failure to communicate impact of non-compliances to decision authority
- Hardware Design
  - Primary explosive in-line in ignition train
  - Non-compliant S&As
  - User interface requirements not met
- Independent Review
  - Funding not allocated for IRs
  - Need not recognized by PO
  - Avoidance of Safety Release Process
- Management
  - Restricted flow of safety information to upper management
  - Allowed deferment of critical safety requirements due to acquisition process
  - No acceptance of residual risks
- Process Control
  - Reliance on Prime Contractor with very limited Government oversight
  - Significant use of "redlined" procedures by developer and user

# DOD Findings

A TRADITION OF EXCELLENCE

- Safety Culture
  - Fractured safety program
  - Safety deemed to have minimal return on investment i.e. not a priority
  - Safety Function did not have access to senior leadership
- Software Design
  - No safety standard levied
  - Dead code not removed
  - Incomplete validation process
  - Limited review of safety critical code
- Test Set-Up
  - Limited "real-world" scenarios
  - Inability to conduct integrated system-level testing due to hardware limitations
- Training
  - Limited or no trainer capability
  - Use of tactical assets for training
  - No requirement for developer to provide training/user manuals
  - User developed training procedures during operational sessions
- Workmanship/Quality Control
  - Lack of flow-down of requirements by Prime contractor to subs
  - Inadequate Government oversight

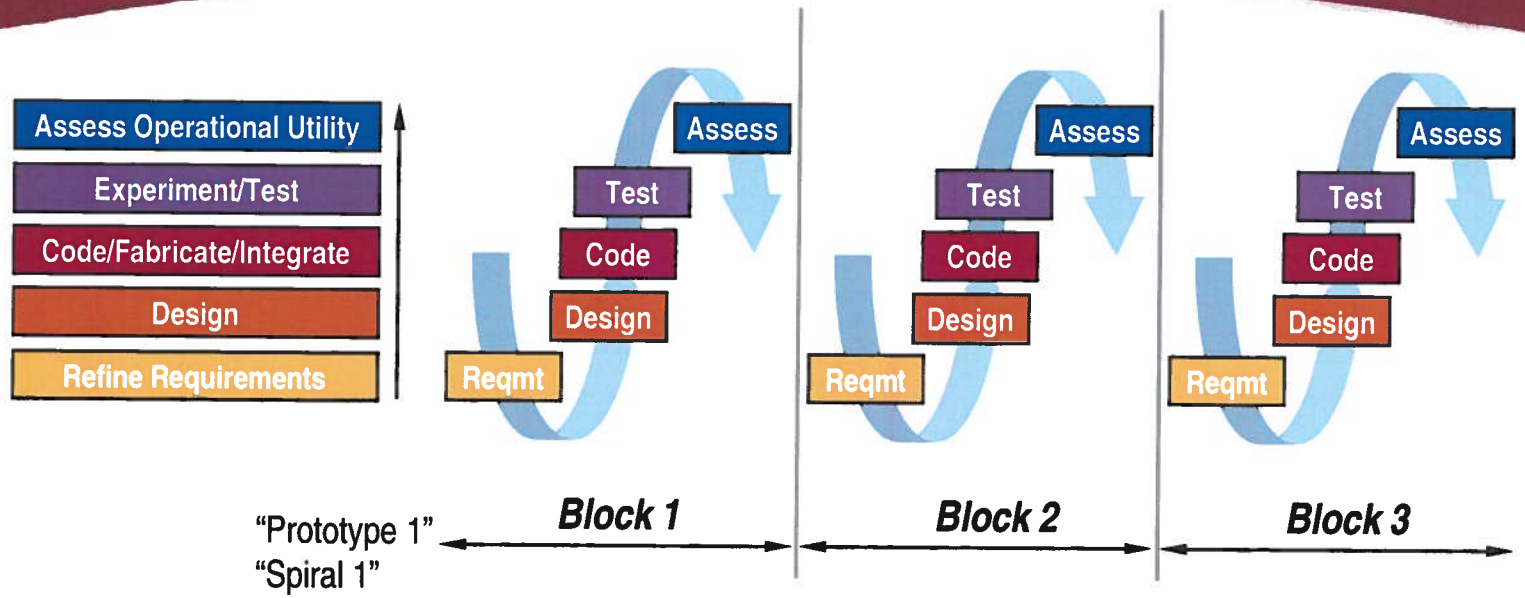
A TRADITION OF EXCELLENCE

- Loss of Personnel & Expertise
- Urgent Material Release
- Decentralization of Risk Acceptance
- Spiral Development
- Budget Shortfalls
- Schedule Pressures

# System Safety

# Spiral Development

A TRADITION OF EXCELLENCE




- Allows *intentional* non-compliance with the standard weapon design and fielding process
- Safety controls that are very invasive to the design must be designed in at the beginning
- Not cost effective to "fix" after fielding or subsequent spirals (re-qual $$, loss of assets available to Warfighter)
- Block 1 items may appear the same as Block 2, 3, etc.
- Level of safety and operational procedures may be significantly different
- Differences may not be apparent to the Warfighter

UNCLASSIFIED

# Safety Status – Urgent Fielding

## — Example —

A TRADITION OF EXCELLENCE

| | |
|---|---|
| **Safety & Health Data Sheet Documentation** | |
| **Safety Assessment Report** (AR 385-16) | |
| **Hazard Analyses** (Mil-Std-882D, AR 385-16) | |
| **System Safety Risk Assessments** (AR 385-16) | |
| **DTC Safety Confirmation** (AR 385-16) | |
| **Health Hazard Assessment Report** (AR 385-16, para 3-16 & AR 40-10) | |
| **Explosive Hazard Classification** (AR 385-16, TB 700-2) | |
| **Surface Danger Area & Range Fan** (AR 385-63, C-7, DA PAM 385-63) | |
| **Army Ignition System Safety Review Board Approval** (MIL-STD 1901) | |
| **Army Fuze Safety Review Board Approval** (STANAG 4187/MIL-STD1316) | |
| **Explosive Ordnance Disposal/DEMIL Procedures** (AR 75-15) | |
| **MANRATING Certification** (MICOMR 385-10) | |
| **Insensitive Munitions Data** (10 CFR, AR 70-3, DA PAM385-64) | |
| **Human Factors Engineering Analysis** (AR 602-1, AR 385-16, MIL-STD-1472) | |
| **E3/EMR** (RDTE 87-1/MIL-STD 6051D | |

Note:
- Requirements Completed
- In-Process to Meet Requirements
- Requirements not Accomplished
- Requirements Not Required at this time

# System Development "On Paper" vs Reality



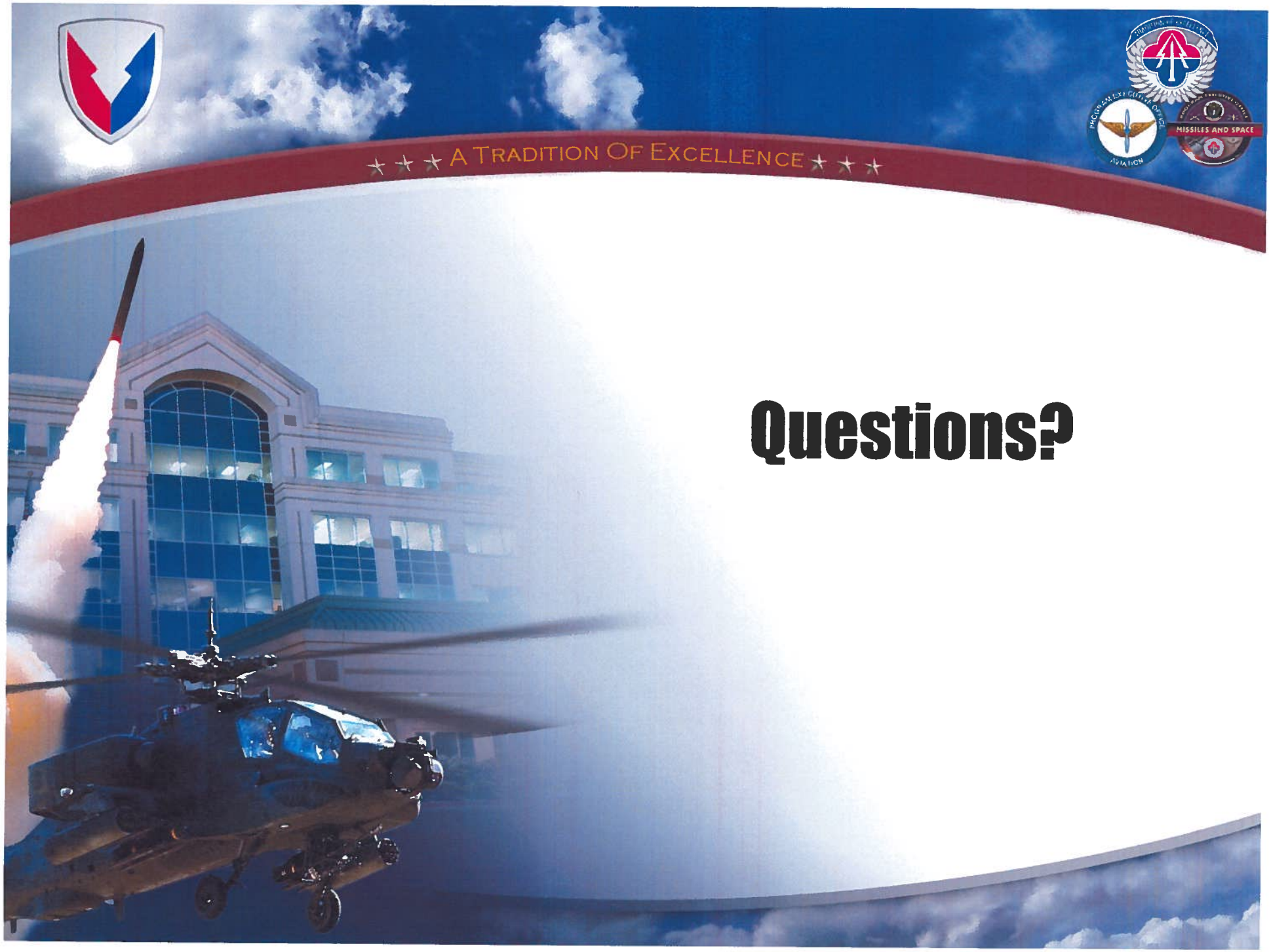
- It is simple.
- It is small.
- It is cheap.
- It is lightweight.
- It can be built very quickly.
- Very little development is required; it can use off-the shelf components.
- It is in the study phase; it is not being built now.

- It is complicated.
- It is large.
- It is expensive.
- It is heavy.
- It takes a long time to build because of its engineering development problems.
- It requires an immense amount of development on apparently trivial items.
- It is being built now.

# Conclusion and Recommendations



- Complexity of today's systems tend to work in safety's favor
- User's mistrust that the system will actually work complicates the hazard message
- Comparison with past systems provides a more tangible understanding of concerns in a spiral development program
- Systems currently in development have seen numerous non-catastrophic incidents
  - Could be seen as an indicator of one or more categories in the general findings
  - Systems have not yet been fielded, therefore have seen only controlled environments and testing – no real stress which could precipitate a serious failure
  - May have time to correct
- This assessment gives the safety engineer another tool for hazard assessment and risk identification


A TRADITION OF EXCELLENCE
MISSILES AND SPACE
Questions?